REMARKS

The Applicants wish to thank the Examiner for reviewing the present application.

Firstly, the Applicants wish to note the change in docket number indicated above. Kindly update the present application accordingly.

The Examiner has rejected claim 23 under 35 U.S.C. 112 second paragraph, as being indefinite. Claim 23 has been amended to refer to steps (d) and (h) instead of step (e). Applicants note that in claim 7 (from which claim 23 depends) a first MAC is computed in step (d) and a second MAC in step (h). Accordingly, claim 23, as amended, refers to "the MACs computed in steps (d) and (h)". Therefore, the Applicants believe that claim 23 complies with 35 U.S.C. 112 second paragraph, and that no new subject matter has been added.

The Applicants wish to note that claim 7 has been amended to correct a clerical error.

The Examiner has also rejected claims 7-16, 22, 27-31, 38-42, and 48 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,153,919 to Reeds, III et al. ("Reeds"); in view of U.S. Reissue Patent No. Re. 36,946 to Diffie et al. ("Diffie"); and further in view of U.S. Patent No. 5,784,463 to Chen et al. ("Chen"). The Applicants respectfully traverse this rejection.

The present application describes a method of authenticating a mobile unit, typically a cell phone, with a base station, that provides mutual authentication and session key establishment with a reasonable assurance of security, while reducing traffic overhead in the system. Mutual authentication is established as follows. Authentication of the mobile unit to the base station is based on the latter having trusted knowledge of the former's public key and authentication of the base station to the mobile unit is based on the latter having trusted knowledge of its private key (both summarized in paragraph [0054] of the application).

Communication traffic on the backbone is reduced because the shared secret data

("SSD") mechanism of the system is not employed, and hence SSDs need not be communicated. The method involves using a Diffie-Hellman calculation to establish a shared secret, from which keys are derived for HMACs and session encryption.

Reeds teaches a mobile telephone registration and authentication system built upon symmetric key techniques. Both the mobile unit and its service provider possess the same symmetric key. The techniques employed include the use of MACs and a home-grown symmetric key cipher. Reeds works within the realm of two-tiered symmetric "A-keys" and "SSDs". Reeds teaches against the use of public key systems for being too efficient in column 2, lines 49-50.

Diffie teaches a mobile telephone registration and authentication system built upon public key techniques and employing certificates and a challenge response protocol.

Chen teaches a secure online registration system built upon public and private key techniques. The client possesses a certificate of the server's public key and registers itself by generating a first symmetric key, encrypting the symmetric key with the base station's public key, and sending the encrypted key to the server. The latter extracts the symmetric key, generates a second symmetric key, and sends back the second symmetric key encrypted with the first symmetric key. At this point, both sides possess both symmetric keys and combine them into a shared secret.

The Examiner has rejected independent claims 7, 27, 38 and 48 for similar reasons. For clarity, the following will address the Examiner's rejection with respect to claim 7.

The Examiner appears to have pieced together teachings found in three separate references in an attempt to find all the elements recited in the claims. Regarding claims 7, the Examiner believes that Reeds teaches steps (d) to (e) and steps (g) to (l) of claim 7, minus a base station identity on which a MAC is computed. As indicated above, Reeds teaches away from the use of public keys and instead teaches the use of A-keys and SSDs. The Examiner has relied

upon column 2, lines 30-31 of Reeds. Although Reeds does mention the use of a pair of RSA keys, if one reads further down column 2, specifically lines 45-50, it is clearly stated by Reeds that his intention is to avoid using public keys as he finds them to be inefficient, and as such, Reeds teaches against the use of public keys.

Therefore, it is believed that it would be improper to combine the teachings of Reeds with the other references relied upon by the Examiner, since Reeds is not even intended to be used in a public key system. In paragraph 58 of the present application, it is clearly stated that public key technology is used in the present application, to avoid using A-keys and sending SSDs. That is in fact exactly what Reeds does. In any case, Reeds does not teach the steps indicated by the Examiner since the text relied on actually teaches against using public key systems. Therefore, the steps recited in the claim cannot be considered part of Reeds' teachings. Therefore, not only does Reeds not teach the steps described in claim 7, it clearly teaches away from the use of a public key system.

The Examiner has relied on Diffie to find an equivalent to steps (a) and (b). Steps (a) and (b) are part of a standard one-pass Diffie-Hellman exchange as indicated in the present application at paragraphs [0051] and [0052]. In the present application, particularly at paragraph [0060], it was clearly stated that the method of the present invention was to incorporate such a Diffie-Hellman exchange. Although Diffie describes a communication system between a base station and a mobile device using public and private key techniques, Diffie does not generate a pair of secret keys to compute MACs as required by steps (c) to (l). Therefore, Diffie does not teach the method recited in claim 7, but merely teaches a small portion thereof (i.e. steps (a) and (b)), which has been identified by the Applicants in the present application, as known in the art.

The Examiner believes that Chen reads on steps (c) to (l) of claim 7. The Examiner has relied on column 3, lines 13-24 of Chen.

As outlined above, Chen teaches a method wherein a first symmetric key is encrypted with the other correspondent's public key, this encrypted key is sent to the other correspondent,

the second correspondent extracts the first key, generates a second symmetric key and encrypts and sends the second key back to the other correspondent. This method is generally described in column 3, lines 13-24 of Chen (as indicated by the Examiner). The Examiner has equated the above to steps (c) and (f) of claim 7. However, step (c) requires that the first correspondent combine its private key with the short-lived public key to generate a pair of secret keys, which are then used individually in subsequent steps. Chen does not teach the generation by one correspondent of a pair of secret keys from a combination of a public key and a private key. This step is missing from Chen.

The two keys generated in the method taught by Chen cannot be equated with those generated in step (c), since each of the two keys generated in Chen are generated by a different correspondent and not by one correspondent as is recited in step (c). Moreover, the use of the keys generated by Chen is entirely different from that claimed. Once the keys are generated by Chen, they are combined to create a shared secret key, which is used for secure exchange thereafter. In claim 7, a first of the secret keys generated in steps (c) or (f) are used to compute a MAC for registering the correspondent and the second of the secret keys used to create session keys. Therefore, not only does Chen not teach a pair of secret keys generated by one correspondent, the keys generated by Chen at different correspondents are combined for subsequent secure exchanges, and not separately used to compute MACs and session keys. Therefore the keys created by Chen are neither allocated within the system nor used in the manner recited in steps (d)-(l) of claim 7.

The Applicants wish to note that the Examiner has made a blanket statement indicating that Chen discloses that a shared secret key can be used for mutual authentication, and this would read on steps (d) to (e) and steps (g) to (j). However, the Examiner does not indicate where in Chen these steps are actually recited. As indicated above, Chen does not teach a single correspondent generating a pair of secret keys, let alone a first of the secret keys being used to compute a MAC and a second of the keys used to generate a session key. It appears that the Examiner has taken a few isolated words from the description of Chen in coming to such a conclusion. Therefore, the Applicants believe that the Examiner has misconstrued the teachings

of Chen, and that the steps recited in claim 7 do not form part of the teachings therein.

In view of the foregoing, it is believed that the combination of Reeds, Diffie, and Chen does not teach all the steps recited in claim 7, nor is combination even a suitable one. Reeds teaches away from using a public key infrastructure and Chen merely describes a key exchange different from step (c), which uses the secret keys in a different manner than that recited in steps (d)-(l). At most, steps (a) and (b) may be described by Diffie, but Diffie also fails to teach any of steps (d)-(l). Therefore, the Applicants believe that even if the combination of Reeds, Diffie, Chen is contemplated, the combination would not teach all the steps recited in claim 7.

Quite clearly, none of the art teaches each of the features recited in claim 7, and therefore cannot anticipate claim 7.

The Examiner has rejected claim 7 under 35 U.S.C. 103 on the basis of Reed in view of Diffie in view of Chen. As noted above, such a combination does not disclose the steps set out in claim 7 and accordingly, cannot render claim 7 obvious.

Moreover, such a combination is improper in light of the teachings of the individual references. Reeds teaches the use of symmetric keys and directs away from the use of public key systems. Diffie however, is entirely concerned with public keys. In light of the disparate teachings and the comments made in Reeds, there is no motivation to combine the teachings and to do so is contrary to the instructions provided to a person skilled in the art by Reeds.

Similarly, Reeds and Chen are directed to disparate technology with clear direction in Reeds not to use the type of system embodied in Chen. Accordingly, there is again no motivation to make such a combination.

Diffie and Chen embody public key technology but each offers alternative techniques for effecting communication. Chen does not offer alternative steps to the overall protocol of Diffie but rather an entirely different protocol. Therefore, the combination of Diffie and Chen would

yield either Diffie or Chen, not a hybrid of both.

Therefore, there is clearly no motivation for the combination suggested by the Examiner, and in any event, such a combination does not yield the invention claimed.

As such, it is believed that claim 7 clearly and patentably distinguishes over the combination of references cited by the Examiner, and is in condition for allowance. Claims 8-26 are either directly or indirectly dependent upon claim 7 and as such, are also believed to distinguish over the combination of Reeds, Diffie, and Chen.

Claim 27 is directed to a base station suitable for implementing the method of claim 7. Therefore, similar arguments apply as per claim 7. Claims 28-37 are either directly or indirectly dependent upon claim 27 and as such are also believed to distinguish over the combination of Reeds, Diffie, and Chen.

Claims 38 and 48, are directed to methods which also are believed to distinguish over the prior art for reasons similar to those presented in favour of claim 7. Claims 39-47 are either directly or indirectly dependent upon claim 38 and as such are also believed to distinguish over the combination of Reeds, Diffie, and Chen.

The Examiner has rejected claims 17-18, 32-33 and 43-44 under 35 U.S.C. 103(a) as being unpatentable over Reeds, in view of Diffie, in view of Chen, and further in view of U.S. Patent No. 5,883,960 to Maruyama et al. (Maruyama). However, Maruyama does not teach the steps of claims 7, 27 and 38 missing from Reeds, Diffie and Chen as outlined above, therefore cannot render claims 17-18, 32-33 and 43-44 obvious.

The Examiner has rejected claims 19-20, 34-35 and 45-46 under 35 U.S.C. 103(a) as being unpatentable over Reeds, in view of Diffie, in view of Chen, and further in view of U.S. Patent No. 6,260,147 to Quick, Jr. (Quick). However, Quick does not teach the steps of claims 7, 27 and 38 missing from Reeds, Diffie and Chen as outlined above, therefore cannot render

claims 19-20, 34-35 and 45-46 obvious.

The Examiner has rejected claims 25 and 37 under 35 U.S.C. 103(a) as being unpatentable over Reeds, in view of Diffie, in view of Chen, and further in view of U.S. Patent No. 6,209,093 to Venkatesan (Venkatesan). However, Venkatesan does not teach the steps of claims 7, 27 and 38 missing from Reeds, Diffie and Chen as outlined above, therefore cannot render claims 25 and 37 obvious.

In summary, it is believed that claims 7-48 as presented in this amendment, clearly and patentably distinguish over the prior art, and as such constitute patentable subject matter and are in condition for allowance.

The Applicants respectfully request early reconsideration and allowance of the present application.

Respectfully submitted,

Ralph A. Dowell
Agent for Applicant
Registration No. 26,868

Date: March 22, 2005

DOWELL & DOWELL, P.C.
Suite 406
2111 Eisenhower Avenue
Alexandria, VA 22314
U.S.A.

Tel: 703-415-2555
JRO/BSL/dm